The Deletion of Data is Often Key Evidence in Proving Facts of a Case

Related Professionals

Whitney C. Gibson

CLIENT ALERT | 3.20.2014

We don't want to pretend to know what happened with Malaysia Airlines Flight 370. Yet, it is hard to ignore the latest evidence in the bizarre March 8 disappearance of the airplane. Various media outlets reported Wednesday morning that investigators discovered data had been deleted from the in-home flight simulator belonging to Captain Zaharie Ahmad Shah. The pilot's motives are unclear and it is presently unknown whether there was any bad intent behind this deleted data.

As investigators work to recover the data, we are reminded that the deletion of data discovered through forensic analysis is something that has played a significant role in many of our cases.

Purposeful Deletion and Forensic Analysis

We have handled several cases in which people have tried to cover their tracks by deleting computer data. They may be able to fully delete electronic information, but evidence suggesting they did delete this relevant information can be discovered through forensic analysis.

We have discovered the timing of the deletion can provide insight critical to a forensic analysis. In our cases, we explore when the pertinent information was erased, and whether or not it was normal practice to make the deletions. This is often the key evidence to establishing who committed the acts in questions.

Another technique we utilize is finding out what type of wiping software had been used. There is certain software designed for people to remove all traces of evidence, which would further suggest someone was attempting to hide the information.

Other Information the Forensic Investigators May Consider

Besides exploring facts related to the deletion, it is also possible in some cases for forensic experts to find pieces related to the deleted information. For instance, forensic investigators may find the file's metadata, which could provide:

- When the file was installed;
- Whether it was modified (and when);
- When it was deleted; and
- Information about the data contained within the file.

If a program or malware was involved, it may be reverse engineered to determine exactly the program's intended purpose.

In short, in addition to conducting a forensic analysis pertaining to deleted data, forensic investigators can often recover portions or all of the deleted data to prove a case.

This article was co-authored by Internet attorney, Whitney Gibson, and cyber investigator, Bruce Anderson. You can contact Whitney Gibson at 855.542.9192 or wcgibson@vorys.com. You can contact Bruce Anderson at bruce@cyberinvestigationservices.com.

Read more about their practices at http://www.internetcrisesattorneys.com and http://www.cyberinvestigationservices.com.